UNITED STATES PATENT AND TRADEMARK OFFICE
DOCUMENT CLASSIFICATION BARCODE SHEET

Page 1 of 1

CATEGORY:

CLEARED

ADDRESS
CONTACT IF FOUND:

09-18-00

A

09/15/00 Jc846 U.S. PTO

NEW, CONTINUATION, DIVISIONAL OR CONTINUATION-IN-PART APPLICATION UNDER 37 C.F.R. §1.53(b)

Attorney Docket No. 9432-000119

Express Mail Label No. EL581380971US

Date September 15, 2000

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

09/662698 Jc918 U.S. PTO 09/15/00

Hon. Commissioner of Patents and Trademarks
Washington, D. C. 20231

Sir:

Transmitted herewith for filing under 37 C.F.R §1.53(b) is a patent application for SECURE SYSTEM AND METHOD FOR ACCESSING FILES IN COMPUTERS USING FINGERPRINTS

identified by: [ ] First named inventor Prabir BHATTACHARYA
or [X] Attorney Docket No. (see above)

1. **Type of Application**

[X] This application is a new (non-continuing) application.

[ ] This application is a [ ] continuation / [ ] divisional / [ ] continuation-in-part of prior application No. ____. Amend the specification by inserting before the first line the sentence:

--This is a [continuation/division/continuation-in-part] of United States patent application No. ____, filed ____.--

[ ] The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied, is considered part of the disclosure of the accompanying application and is hereby incorporated by reference therein.

If for some reason applicant has not requested a sufficient extension of time in the parent application, and/or has not paid a sufficient fee for any necessary response in the parent application and/or for the extension of time necessary to prevent the abandonment of the parent application prior to the filing of this application, please consider this as a Request for an Extension for the required time period and/or authorization to charge our Deposit Account No. 08-0750 for any fee that may be due. THIS FORM IS BEING FILED IN TRIPLICATE: one copy for this application; one copy for use in connection with the Deposit Account (if applicable); and one copy for the above-mentioned parent application (if any extension of time is necessary).

2. **Contents of Application**

a. Specification of 13 pages;
[ ] A microfiche computer program (Appendix);
[ ] A nucleotide and/or amino acid sequence submission;

[ ] Because the enclosed application is in a non-English language, a verified English translation [ ] is enclosed [ ] will be filed.

[ ] Cancel original claims ____ of the prior application before calculating the filing fee. (At least one original independent claim must be retained for filing date purposes.)

b. [X] Drawings on 3 sheets;

c. [X] A signed Oath/Declaration [X] is enclosed / [ ] will be filed in accordance with 37 C.F.R. §1.53(f).

The enclosed Oath/Declaration is [X] newly executed / [ ] a copy from a prior application under 37 C.F.R. §1.63(d) / [ ] accompanied by a statement requesting the deletion of person(s) not inventors in the continuing application.

d. **Fees**

FILING FEE CALCULATION	Number Filed		Number Extra		Rate		Basic Fee $690.00
Total Claims	23	- 20 =	3	×	$18.00	=	$54.00
Independent Claims	2	- 3 =	0	×	$78.00	=	.00
Multiple Dependent Claim(s) Used					$260.00	=	
FILING FEE - NON-SMALL ENTITY							$744.00
FILING FEE - SMALL ENTITY: Reduction by 1/2 [ ] Verified Statement under 37 C.F.R. §1.27 is enclosed. [ ] Verified Statement filed in prior application.							
Assignment Recordal Fee ($40.00)							$40.00
37 C.F.R. §1.17(k) Fee (non-English application)							
TOTAL							**$784.00**

[X] A check is enclosed to cover the calculated fees. The Commissioner is hereby authorized to charge any additional fees that may be required, or credit any overpayment, to Deposit Account No. 08-0750. A duplicate copy of this document is enclosed.

[ ] The calculated fees will be paid within the time allotted for completion of the filing requirements.

[ ] The calculated fees are to be charged to Deposit Account No. 08-0750. The Commissioner is hereby authorized to charge any additional fees that may be required, or credit any overpayment, to said Deposit Account. A duplicate copy of this document is enclosed.

3. **Priority Information**

[ ] **Foreign Priority**: Priority based on _____ Application No. _____, filed _____, is claimed.

[ ] A copy of the above referenced priority document [ ] is enclosed / [ ] will be filed in due course, pursuant to 35 U.S.C. §119(a)-(d).

[ ] **Provisional Application Priority**: Priority based on United States Provisional Application No. ____, filed ____, is claimed under 35 U.S.C. §119(e).

Attorney Docket No. 9432-000119

Express Mail Label No. EL581380971US

Date September 15, 2000

4. **Other Submissions**

[ ] A Preliminary Amendment is enclosed.

[ ] An Information Disclosure Statement, ____ sheets of PTO Form 1449, and ____ patent(s)/publications/documents are enclosed.

[X] A power of attorney

[X] is submitted [X] with the new Oath/Declaration.

[ ] is of record in the prior application and [ ] is in the original papers / [ ] a copy is enclosed.

[X] An Assignment of the invention

[X] is enclosed with a cover sheet pursuant to 37 C.F.R. §§3.11, 3.28 and 3.31.

[ ] is of record in a prior application. The assignment is to ____, and is recorded at Reel ____, Frame(s) ____.

[ ] An Establishment of Assignee's Right To Prosecute Application Under 37 C.F.R. §3.73(b), and Power Of Attorney is enclosed.

[X] An Express Mailing Certificate is enclosed.

[ ] Other: _____

_____

Attention is directed to the fact that the correspondence address for this application is:

Harness, Dickey & Pierce, P.L.C.
P.O. Box 828
Bloomfield Hills, Michigan 48303
(248) 641-1600.

Respectfully,

Date September 15, 2000

Gregory Stobbs

Gregory A. Stobbs
Reg. No. 28,764

Harness, Dickey & Pierce, P.L.C.
P.O. Box 828
Bloomfield Hills, Michigan 48303
(248) 641-1600

HARNESS, DICKEY & PIERCE, P.L.C.
ATTORNEYS AND COUNSELORS
P.O. BOX 828
BLOOMFIELD HILLS, MICHIGAN 48303
U.S.A.

TELEPHONE
(248) 641-1600

TELEFACSIMILE
(248) 641-0270

Date September 15, 2000

Hon. Commissioner of Patents
and Trademarks
Washington, D.C. 20231

Sir:

EXPRESS MAILING CERTIFICATE

Applicant: Prabir BHATTACHARYA

Serial No : not yet assigned

For: SECURE SYSTEM AND METHOD FOR ACCESSING FILES IN COMPUTERS USING FINGERPRINTS

Docket: 9432-000119

Attorney: Gregory A. Stobbs

"Express Mail" Mailing Label Number ..... EL581 380 971 US

Date of Deposit ..... September 15, 2000

I hereby certify and verify that the accompanying acknowledgement postcard, Check in the amount of $784.00 ($690.00-Basic Filing Fee, 3-excess Total Claims $54.00, $40.00-Assignment Recordal fee), Transmittal letter (In Duplicate), 13-page Patent Application; 3 sheets of drawings showing Figs 1-5; executed Declaration/Power of Attorney, cover sheet for recordal of assignment (in Duplicate) and Assignment are being deposited with the United States Postal Service "Express Mail Post Office To Addressee" service under 37 C.F.R. 1.10 on the date indicated above and (is) are addressed to the Commissioner of Patents and Trademarks, Washington, D.C. 20231.

Pamela Strauss

Signature of Person Mailing Document(s)

SECURE SYSTEM AND METHOD FOR ACCESSING FILES IN COMPUTERS USING FINGERPRINTS

Background and Summary of the Invention

The present invention relates generally to computer access systems and file access systems. More particularly, the invention relates to a system and method to attach different authorization levels to computer files resources which are then accessed by the user's fingerprint. The computer or computer system includes a touch pad to which the user inputs his/her fingerprint. The touch pad can also serve as an input device for cursor control.

Computer security has become an important topic, particularly in view of the widespread use of computers and the Internet. Most computer users are familiar with the traditional user ID and password as a security mechanism for logging onto a computer system, and optionally for gaining access to certain secure files. One problem, of course, is that user IDs and passwords are subject to security attack. User IDs and passwords can be guessed. Some users even employ the unrecommended practice of writing their passwords on a note placed near the computer for easy access, not only by themselves, but also by unauthorized interlopers. In a network computer environment, some users will walk away from their computer or workstation, leaving the system logged on where any other person may gain access to the computer network by simply borrowing the other person's computer. Some computer application programs are even designed to store user ID and passwords, so that the user does not need to type them every time the computer is used. This can make the computer a potential security risk. Laptop computers are particularly vulnerable, cause they are frequently carried to insecure locations, such as airport terminals, where they are more likely to be stolen.

In the interest of addressing the above security issues, the present invention employs a fingerprint reading device that the computer user must first touch before

access to the computer or to protected files or computer resources are granted. In one embodiment, the touch pad is integrated with the cursor control touch pad, making the embodiment ideal for laptop computers. The system maintains a data store of authorized user fingerprints, which may be stored in an encrypted form. A pattern matching algorithm compares the user's fingerprint, entered through the touch pad, with the fingerprint data in the data store, utilizing a decryption module to access the data as needed. The user's identity is then either identified from the fingerprint or verified from the fingerprint and a user authorization level is attached to the user ID for the file resource operation requested by the user. The authorization level data may also be encrypted, making it more difficult for a computer hacker to mimic the fingerprint pattern matching operation. The user's ID and authorization level information is then sent to an access module which causes the operating system to grant access to the file resources requested by the user. The access module also utilizes the decryption modules services, as required, to decrypt the authorization level generated during the authorization level assignment.

The system is configured so that it is resistant to tampering or attack by hackers. In its most secure form, each module operates using encrypted data and stores its output data in an encrypted form designed only to be read by other modules within the system with a need to utilize the information. The system is thus designed to make it difficult for hackers to spoof a given module by supplying data that mimics the output of another module. This security feature allows the system to be implemented across a network, if desired. Thus, although the fingerprint reading device may be physically embodied in the computer, or in the computer cursor control or keyboard, the fingerprint reading device may alternatively be used in a network environment where the computer being accessed is located remote from the reading device.

The invention allows the user's fingerprint to serve as either the user's

identification indicia, or the user's password indicia, or both. If desired, conventional text-based user ID and passwords can be used along with the user's fingerprint for added security. The user's fingerprint can be used not only to access files but also other computer system resources. In one embodiment, the computer resource can be a hyperlink on a web page. The system denies access to that hyperlink unless the user's fingerprint is on the authorized list. In an embodiment that uses the computer touch pad for both cursor control and fingerprint identification, the system allows the authorized user to manipulate the cursor to the desired hyperlink and open the link, whereas unauthorized users will not be able to open the link. In some systems the user's fingerprint can be used for basic log on identification. In other more secure applications, the user's fingerprint may be required for specific file access or specific record access, or for specific computer resource access each time access is requested. For a more complete understanding of the invention, its objects and advantages, refer to the following specification and to the accompanying drawings.

Brief Description of the Drawings

Figure 1 is a system plan view illustrating implementation examples of the invention; and

Figure 2 is a system block diagram and data flow diagram illustrating a presently preferred embodiment of the invention.

Description of the Preferred Embodiments

The secure system and method for accessing computer resources and file resources can be implemented in a variety of different ways. Figure 1 illustrates several of these. With a laptop computer **10** the fingerprint reading device may be incorporated into the touch pad **12** designed for cursor control. In a computer workstation or desktop computer **14**, the fingerprint reading device **16** may be a separate scanning unit attached by cable to the computer. Any of the computers can be attached to a computer network **18**, such as the Internet, allowing them to communicate with remote server computers such as computer **20**. As will be more fully explained below, the fingerprint reading mechanism can be integrated into a security system that spans network **18**. Thus, the touch pad **12** for scanner **16** may be used in some embodiments to allow a user at the laptop **10** or workstation **14** to access resources on server **20**. Thus, while the fingerprint security mechanism of the invention is well-suited for imposing security over local computer systems, the principles of the invention can readily be extended to network systems spanning the globe.

Referring to Figure 2, a presently preferred embodiment of the system is illustrated. Authorized user fingerprint data is stored in a suitable memory, preferably in an encrypted form. The authorized user fingerprint data is captured by a learning or training process whereby the user places his or her finger on a touch pad fingerprint scanner and the fingerprint is then digitized and converted to feature parameters representing the unique aspects of that person's fingerprint. The authorized user fingerprint data is then accessed by a pattern matching module **42** when the system is used. In such use the person wishing to gain access to computer resources places his or her finger on the touch pad scanner **16** and the user's fingerprint is thus digitized and parameterized using the same techniques that were employed during the original training operation. The pattern matching module

42 then compares the user's fingerprint data with data stored at **40**, to determine whether a match can be found. The presently preferred pattern matching module is capable of performing both fingerprint authentication and fingerprint identification. Authentication involves a process whereby the user's identification is asserted, such as through a conventional log in process. The fingerprint is then used to verify or authenticate that the asserted user is in fact genuine. The identification process is related but somewhat different. In the identification process, the user's identity is not known and the fingerprint is thus used to ascertain the identity of the unknown user.

The presently preferred, more secure, embodiment uses encryption at each interface between modules. Thus the information stored at **40** is encrypted and must be decrypted by the pattern matching module **42** in order for that module to use the information. Of course, a less secure embodiment can also be implemented, in which case the fingerprint data need not be encrypted and the pattern matching module can access the data without performing decryption steps. In the illustrated embodiment, a decryption services module **44** provides decryption functionality to the pattern matching module **42**. In other words, the pattern matching module uses the resources of the decryption services module **44** in decrypting the fingerprint data stored at **40**. As illustrated, the decryption services module **42** can be used by other modules as well. Alternatively, each module can embed its own decryption service routines.

The pattern matching module outputs an indicia designating the authenticated identity of a user. In the presently preferred, most secure, embodiment, the authenticated user indicia is also encrypted to make it more difficult for hackers to mimic the output of the pattern matching module and thereby gain access to resources without authorization. The authenticated user identification indicia is used by the authorization module **46** to associate with the authenticated user a given authorization level. In the illustrated embodiment, the authorization module **46**

accesses a data store **48** which contains a list of user authorization level information. Although there are a variety of different ways to assign authorization levels, a presently preferred embodiment uses a hierarchical authorization level as illustrated in Figure 3. Resources at the lowest security level are designated as "unclassified", with higher levels of security being "confidential", "secret", and "top secret." Users having "top secret" authorization level would be permitted to utilize all resources within the computer system. Users with a "secret" authorization level would have access to a subset of resources available to the person with "top secret" clearance. Users with both "confidential" authorization level would, in turn, have access to a subset of what a person with "secret" authorization level would have. Finally, users with an "unclassified" authorization level would have access to a subset of only what persons with a "confidential" authorization level would have. Thus, as illustrated in Figure 3, the person with "top secret" authorization level is able to access the entire block of computer system resources **100**. Each of the succeeding sub-levels would have access to an increasingly smaller portion of those resources.

The authorization module associates an authorization level with a given user, as identified by the pattern matching module **42**. Thus the user authorization level data store **48** may contain a list of user identifiers and their associated authorization level. A suitable data structure for data store **48** is illustrated in Figure 4, where exemplary data has been given for a plurality of users. The authorization module **46** accesses data store **48** to obtain the user's authorization level and associate it with the user's identifier. This information is then transferred to the resource access module **50**. In the presently preferred, most secure, embodiment, the information communicated from authorization module **46** to access module **50** may also be encrypted. The authorization module **46** and access module **50** both utilize the decryption services module **44** in this regard.

The resource access module **50** has an associated data store **52** where

resource authorization level data is stored. Figure 5 shows an exemplary data structure that would be suitable for storing authorization levels associated with individual computer file resources, feature resources and system resources. In Figure 5, exemplary file resources are illustrated at **102**, exemplary system resources at **104** and an exemplary feature resource at **106**. Associated with each resource is the authorization level required to gain access to that resource. Thus using the exemplary data illustrated, a person would require "top secret" authorization level to open the file identified as "secret_data.doc." Similarly, a person would require "secret" authorization level in order to use the print function within the operating system. A person would require "top secret" authorization level to utilize the export feature of a program.

The resource access module **50** uses its data store **52** to determine what authorization level is required to use a particular resource. Module **50** is supplied the authorization level of the user by module **46**, preferably in encrypted form. The resource access module thus determines the user's authorization level and ascertains from its data store **52** whether that user is authorized to utilize the desired resource. The resource access module **50** in turn communicates with the computer operating system to provide resource access to a variety of different resources as illustrated at **54**. The list of features illustrated at **54** is intended to be exemplary and not exhaustive of all possible resources with which this system may be used.

From the foregoing it will be appreciated that the present invention can be implemented in a variety of different configurations, using different fingerprint reading mechanisms and different file structures. Although the preferred embodiment has been illustrated using encryption for all inter-modular communication, other systems are envisioned which would not require encryption between modules as illustrated. In addition, while a single fingerprint has been illustrated here, more advanced systems may utilize multiple fingerprints, such as multiple fingers of the user's hand

or hands. Moreover, if desired, the system can be implemented to introduce a refresh cycle that would require the user to rescan his or her fingerprint at predetermined time intervals to increase security. It should also be apparent that the functions provided by the modules illustrated in Figure 2 can be implemented in different ways, possibly combining several functions into a single module. Also, it should be apparent that communication from one module to another may be effected across a network connection such as across the Internet. Thus, for example, the touch pad scanner **16** and pattern matching module **42** might be physically located in one computer while the authorization module **46** might be located in yet another computer. The resource access module **50** could, in turn, be located in a third computer or in any of the preceding computers. Thus, if desired, the authorization module **46** functionality could be implemented via an Internet connection with the pattern matching module **42** functionality and the resource access module **50** functionality being located at the local user's workstation. Of course, other physical layouts and modular distributions are also possible within the scope of the invention.

While the invention has been described in its presently preferred embodiments, it will be appreciated that the invention is capable of implementation in a variety of different ways without departing from the spirit of the invention as set forth in the appended claims.

Claims

1. A secure computer resource access system, comprising:

a fingerprint reading device;

a store of fingerprint data corresponding to a plurality of different users;

an authorization system coupled to said reading device and configured to access said store and to associate an authorization level with a user based on the user's fingerprint;

an access mechanism that defines a plurality of different authorization levels associated with a plurality of file resources;

said access mechanism being responsive to said authorization system to control how a user can interact with said computer resource based on said associated authorization level.

2. The access system of claim 1 wherein said fingerprint reading device is integral with a pointing device of a computer system.

3. The access system of claim 1 wherein said fingerprint reading device is integral with a keyboard device of a computer system.

4. The access system of claim 1 wherein said store of fingerprint data employs a data structure for storing said fingerprint data in an encrypted format.

5. The access system of claim 4 wherein said encrypted format is protected by a software key.

6. The access system of claim 1 wherein said authorization system communicates with said store of fingerprint data across an encrypted channel.

7. The access system of claim 1 wherein said authorization system communicates with said store of fingerprint data across a computer network.

8. The access system of claim 1 wherein said access mechanism controls file access within a computer system.

9. The access system of claim 1 wherein said access mechanism controls network access within a computer system.

10. The access system of claim 1 wherein said access mechanism controls record access within a computer system.

11. The access system of claim 1 wherein said access mechanism controls resource access within a computer system.

12. The access system of claim 1 wherein said access mechanism controls feature access within a computer system.

13. A method of operating a computer system, comprising:

scanning the fingerprint of a user to generate user fingerprint data;

using said user fingerprint data to access a database of stored fingerprint data and to compare said user fingerprint data with stored fingerprint data;

assigning an access authorization datum to said user based on the results of said comparing step;

controlling how the user can interact with said computer system based on said assigned authorization datum.

14. The method of claim 13 wherein said step of using said user fingerprint data is performed across an encrypted channel.

15. The method of claim 13 wherein said scanning step is performed using a reading device that is integral with a pointing device of said computer system.

16. The method of claim 13 wherein said scanning step is performed periodically as the user interacts with said computer system.

17. The method of claim 13 wherein said scanning step is performed in response to a predetermined action taken by the user in interacting with said computer system.

18. The method of claim 17 wherein said predetermined action is a pointing device action taken by the user through operation of a reading device that is integral with a pointing device of said computer.

19. The method of claim 13 wherein said controlling step includes controlling network access in a computer system.

20. The method of claim 13 wherein said controlling step includes controlling file access in a computer system.

21. The method of claim 13 wherein said controlling step includes controlling record access in a computer system.

22. The method of claim 13 wherein said controlling step includes controlling resource access in a computer system.

23. The method of claim 13 wherein said controlling step includes controlling feature access in a computer system.

Abstract

The user's fingerprint is analyzed by the pattern matching module which draws upon pre-stored fingerprint data that may be encrypted. The pattern matching module works in conjunction with an authorization module and resource access module to ascertain a user's authorization level or security level and then give the user access to only those computer resources for which he or she has been granted authorization. The system preferably employs inter-modular encryption so that the system can be distributed across a network if desired.

Best Available Copy

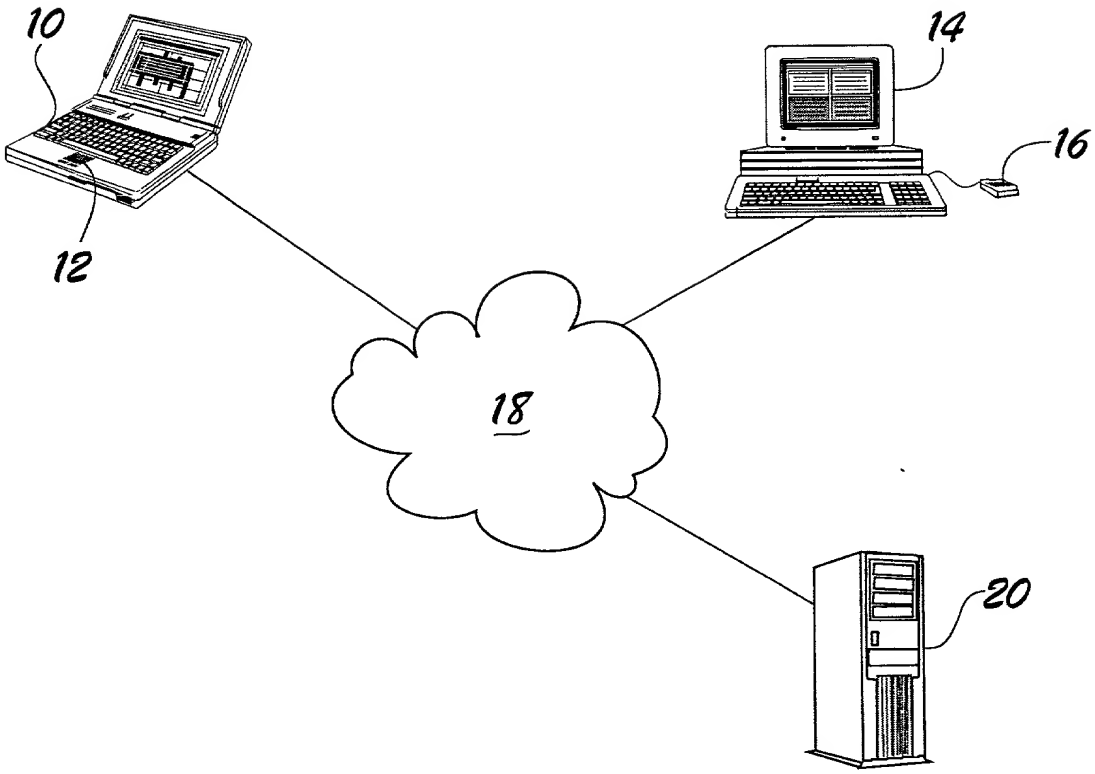

FIG. 1

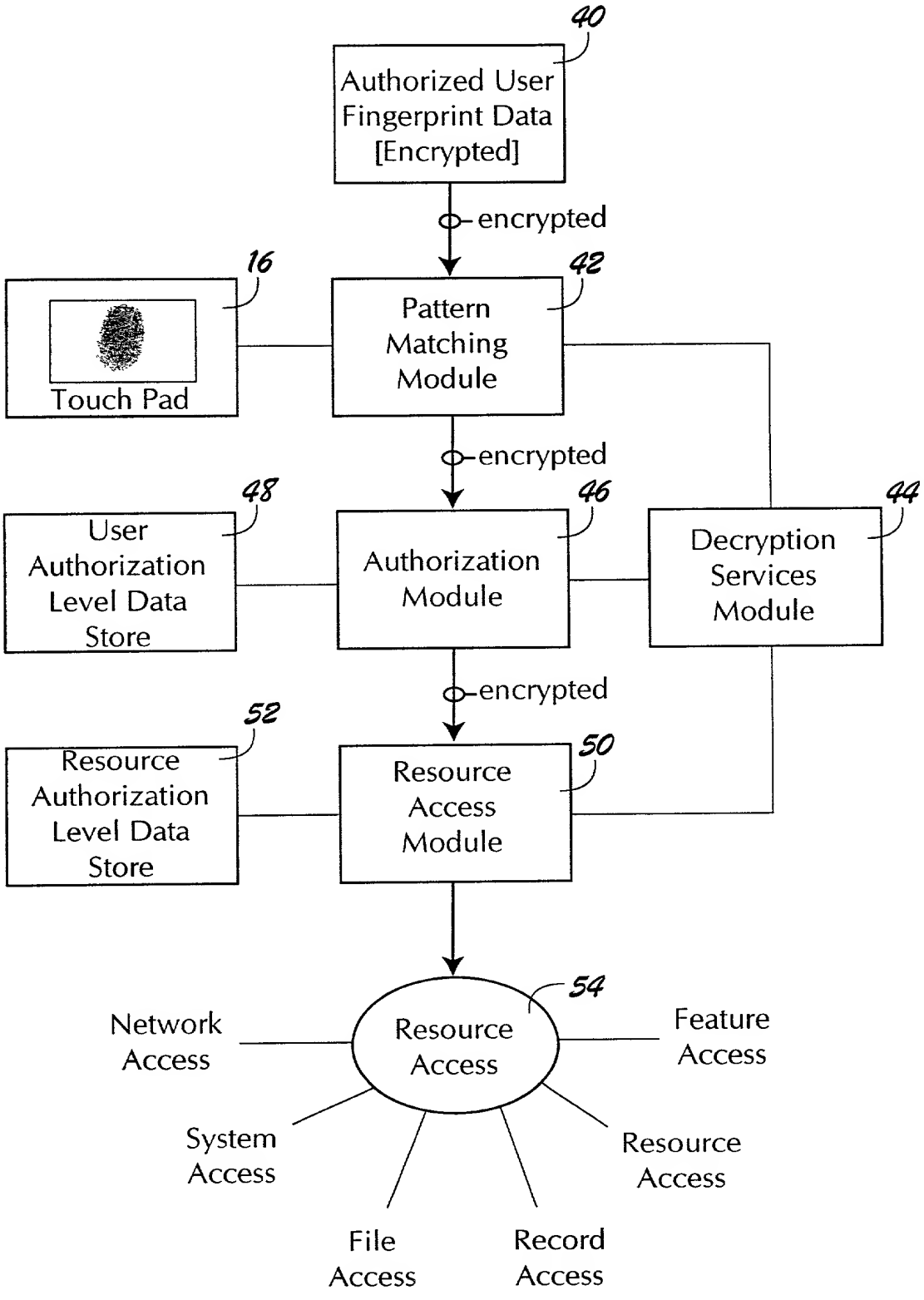
40
Authorized User Fingerprint Data [Encrypted]
encrypted
16
Touch Pad
42
Pattern Matching Module
encrypted
48
User Authorization Level Data Store
46
Authorization Module
44
Decryption Services Module
encrypted
52
Resource Authorization Level Data Store
50
Resource Access Module
54
Network Access
Resource Access
Feature Access
System Access
Resource Access
File Access
Record Access

FIG. 2

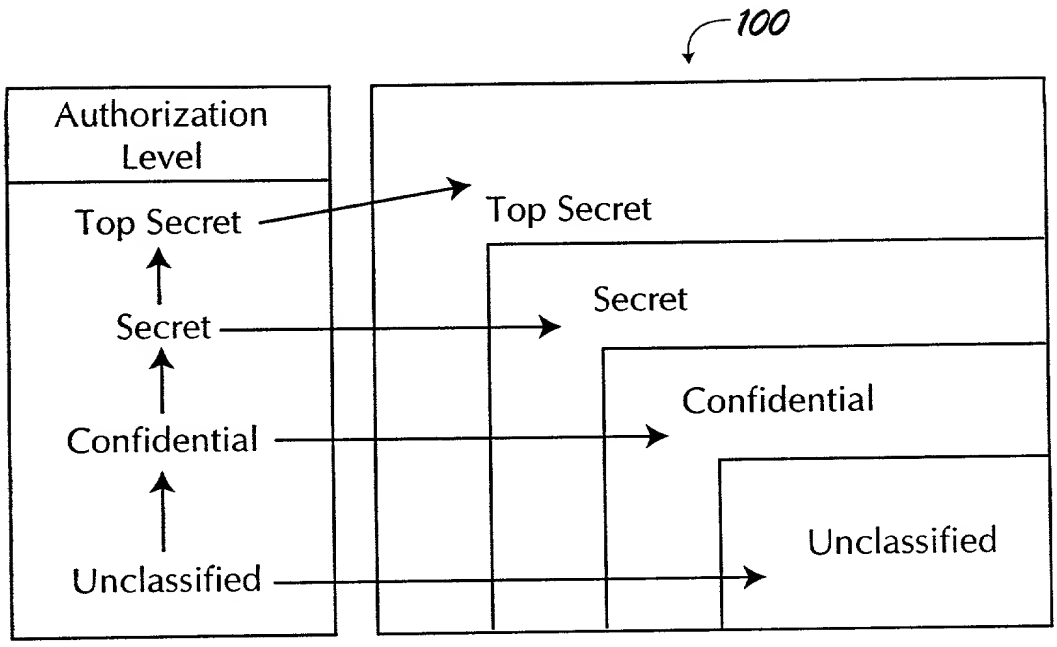

FIG. 3

User ID	Authorization Level
User A	Top Secret
User B	Unclassified
User C	Secret
User D	Secret
.	.
.	.
.	.
User N	Unclassified

FIG. 4

	Resource ID	Authorization Level Required
102	secret_data.doc	Top Secret
102	grocery_list.doc	Unclassified
	.	
	.	
104	print function	Secret
104	save function	Confidential
	.	
	.	
106	export feature	Top Secret

FIG. 5

Microsoft Corporation

Attorney Docket No. 9432-000119

DECLARATION AND POWER OF ATTORNEY

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled

Secure System and Method
for Accessing Files in Computers Using Fingerprints

the specification of which (check one)

[X] is attached hereto.

[ ] was filed on _____ as Application Serial No. _____ and was amended on _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the examination of this application or to the patentability of the invention claimed therein in accordance with Title 37, Code of Federal Regulations, section 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, section 119(a)-(d) of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

PRIOR FOREIGN APPLICATION(S)

			Priority Claim	
(Number)	(Country)	(Day/Month/Year filed)	Yes	No
(Number)	(Country)	(Day/Month/Year filed)	Yes	No
(Number)	(Country)	(Day/Month/Year filed)	Yes	No

DECLARATION AND POWER OF ATTORNEY

I hereby claim the benefit under Title 35, United States Code, §119(e) of any United States Provisional application(s) listed below:

PRIOR PROVISIONAL APPLICATIONS

_____ _____
(application serial number) (Month / Day / Year filed)

_____ _____
(application serial number) (Month / Day / Year filed)

I hereby claim the benefit under Title 35, United States Code, section 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, section 112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, section 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

Application Serial No.	**Filing Date**	**Status – patented, pending, abandoned**

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

I hereby appoint Gregory A. Stobbs, Reg. No. 28,764, and each principal, attorney of counsel, associate and employee of Harness, Dickey & Pierce, P.L.C., who is a registered Patent Attorney, my attorney with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith. I request the Patent and Trademark Office to direct all correspondence and telephone calls relative to this application to Harness, Dickey & Pierce, P.L.C., P. O. Box 828, Bloomfield Hills, Michigan 48303 (248) 641-1600.

Full name of sole or first inventor: Prabir Bhattacharya

Inventor's signature: Prabir Bhattacharya

Date: 9/13/00

Residence: 39 BIRCH DRIVE, PLAINSBORO, NJ 08536

Citizenship: U.S.A.

Post Office Address: 12 Schalks Crossing Rd, Plainsboro 08536